IN THE CLAIMS:

Amended claims follow:

1. (Currently Amended) A method for detecting viruses in software, comprising:

(a) comparing subject data with a plurality of virus definitions in a first database;

(b) executing a security event if the subject data is successfully compared with at least one of the virus definitions;

(c) comparing the subject data with fingerprints of innocent data in a second database;

(d) allowing access to the subject data if the subject data is successfully compared to the fingerprints of innocent data; ~~and~~

(e) transmitting information to a server for analysis purposes if the subject data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data;

(f) comparing the fingerprint associated with the subject data and fingerprints associated with innocent data in a third database at the server;

(g) comparing the fingerprint associated with the subject data and fingerprints associated with virus definitions in a fourth database at the server; and

(h) transmitting the subject data to the server utilizing a network upon an unsuccessful comparison of the fingerprint associated with the subject data and fingerprints associated with the innocent data in the third database and the virus definitions in the fourth database at the server;

wherein the information transmitted to the server includes at least one of the subject data and a fingerprint associated with the subject data;

wherein the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.

2. (Previously Amended) The method as recited in claim 1, wherein the security event is selected from the group consisting of cleaning the subject data, quarantining the subject data, and blocking the subject data.

3. (Previously Amended) The method as recited in claim 1, and further comprising reporting that the subject data is innocent if the subject data is successfully compared to the fingerprints of innocent data.

4.-7. (Cancelled)

8. (Currently Amended) The method as recited in claim ~~7~~1, wherein the third and fourth databases are updated more frequently than the first and second databases.

9. (Cancelled)

10. (Currently Amended) The method as recited in claim ~~9~~1, and further comprising analyzing the subject data transmitted to the server.

11. (Currently Amended) The method as recited in claim ~~9~~1, wherein the subject data is transmitted to the server in separate parts.

12. (Original) The method as recited in claim 10, and further comprising updating at least one of the first database, the second database, the third database, and the fourth database based on the analysis.

13. (Original) The method as recited in claim 1, wherein the information is transmitted to the server via the Internet.

14. (Previously Amended) The method as recited in claim 1, wherein the first database and the second database are both components of a client computer coupled to the server via a network.

15. (Currently Amended) A computer program product for detecting viruses in software, comprising:

(a) computer code for comparing subject data with a plurality of virus definitions in a first database;

(b) computer code for executing a security event if the subject data is successfully compared with at least one of the virus definitions;

(c) computer code for comparing the subject data with fingerprints of innocent data in a second database;

(d) computer code for allowing access to the subject data if the subject data is successfully compared to the fingerprints of innocent data; ~~and~~

(e) computer code for transmitting information to a server for analysis purposes if the subject data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data;

(f) computer code for comparing the fingerprint associated with the subject data and fingerprints associated with innocent data in a third database at the server;

(g) computer code for comparing the fingerprint associated with the subject data and fingerprints associated with virus definitions in a fourth database at the server; and

(h) computer code for transmitting the subject data to the server utilizing a network upon an unsuccessful comparison of the fingerprint associated with the subject data and fingerprints associated with the innocent data in the third database and the virus definitions in the fourth database at the server;

wherein the information transmitted to the server includes at least one of the subject data and a fingerprint associated with the subject data;

wherein the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.

16. (Previously Amended) The computer program product as recited in claim 15, wherein the security event is selected from the group consisting of cleaning the subject data, quarantining the subject data, and blocking the subject data.

17. (Previously Amended) The computer program product as recited in claim 15, and further comprising computer code for reporting that the subject data is innocent if the subject data is successfully compared to the fingerprints of innocent data.

18.-21. (Cancelled)

22. (Currently Amended) The computer program product as recited in claim ~~21~~15, wherein the third and fourth databases are updated more frequently than the first and second databases.

23. (Cancelled)

24. (Currently Amended) The computer program product as recited in claim ~~23~~15, and further comprising computer code for analyzing the subject data transmitted to the server.

25. (Previously Amended) The computer program product as recited in claim 24, wherein the subject data is transmitted to the server in separate parts.

26. (Original) The computer program product as recited in claim 24, and further comprising computer code for updating at least one of the first database, the second database, the third database, and the fourth database based on the analysis.

27. (Original) The computer program product as recited in claim 15, wherein the information is transmitted to the server via the Internet.

28. (Previously Amended) The computer program product as recited in claim 15, wherein the first database and the second database are both components of a client computer coupled to the server via a network.

29. (Currently Amended) A system for detecting viruses in software, comprising:

(a) logic for comparing subject data with a plurality of virus definitions in a first database;

(b) logic for executing a security event if the subject data is successfully compared with at least one of the virus definitions;

(c) logic for comparing the subject data with fingerprints of innocent data in a second database;

(d) logic for allowing access to the subject data if the subject data is successfully compared to the fingerprints of innocent data; ~~and~~

(e) logic for transmitting information for analysis purposes if the subject data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data;

(f) logic for comparing the fingerprint associated with the subject data and fingerprints associated with innocent data in a third database;

(g) logic for comparing the fingerprint associated with the subject data and fingerprints associated with virus definitions in a fourth database; and

(h) logic for transmitting the subject data to the server utilizing a network upon an unsuccessful comparison of the fingerprint associated with the subject data and fingerprints associated with the innocent data in the third database and the virus definitions in the fourth database;

wherein the transmitted information ~~transmitted to the server~~ includes at least one of the subject data and a fingerprint associated with the subject data;

wherein the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.

30. (Currently Amended) A method for detecting viruses in software, comprising:

(a) comparing subject data with a plurality of virus definitions in a first database;

(b) executing a security event if the subject data is successfully compared with at least one of the virus definitions;

(c) comparing the subject data with fingerprints of innocent data in a second database;

(d) reporting that the subject data is innocent if the subject data is successfully compared to the fingerprints of innocent data; and

(e) transmitting the subject data over a network for analysis purposes if the subject data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data;

(f) comparing a fingerprint associated with the subject data and fingerprints associated with innocent data in a third database;

(g) comparing the fingerprint associated with the subject data and fingerprints associated with virus definitions in a fourth database; and

(h) transmitting the subject data to the server utilizing a network upon an unsuccessful comparison of the fingerprint associated with the subject data and fingerprints associated with the innocent data in the third database and the virus definitions in the fourth database;

wherein the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.

31. (Previously Amended) A method for detecting viruses in software, comprising:

(a) receiving a fingerprint associated with subject data from a client computer for analysis purposes upon the subject data being unsuccessfully compared to virus definitions and fingerprints of innocent data stored on the client computer;

(b) comparing the fingerprint associated with the subject data and the fingerprints associated with innocent data at a server;

(c) comparing the fingerprint associated with the subject data and fingerprints associated with virus definitions at the server;

(d) requesting the subject data from the client computer utilizing a network upon an unsuccessful comparison of the fingerprint associated with the subject data, and

the fingerprints associated with the innocent data and the virus definitions at the server;

(e) receiving the subject data transmitted from the client computer in response to the request;

(f) analyzing the subject data transmitted from the client computer; and

(g) updating at least one of the virus definitions and the fingerprints of innocent data based on the analysis;

wherein the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.

32. (Previously Amended) A method for detecting viruses in software, comprising:

(a) receiving a fingerprint associated with subject data from a client computer for analysis purposes upon the subject data being unsuccessfully compared to virus definitions stored on the client computer;

(b) comparing the fingerprint associated with the subject data and fingerprints associated with virus definitions at a server;

(c) requesting the subject data from the client computer utilizing a network upon an unsuccessful comparison of the fingerprint associated with the subject data, and the fingerprints associated with the virus definitions at the server;

(d) receiving the subject data transmitted from the client computer in response to the request;

(e) analyzing the subject data transmitted from the client computer; and

(f) updating the virus definitions based on the analysis;

wherein the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.

33. (Previously Amended) A security method, comprising:

(a) receiving a fingerprint associated with subject data from a client computer for analysis purposes upon the subject data being unsuccessfully compared to fingerprints associated with innocent data stored on the client computer;

(b) comparing the fingerprint associated with the subject data, and fingerprints associated with innocent data at a server;

(c) requesting the subject data from the client computer utilizing a network upon an unsuccessful comparison of the fingerprint associated with the subject data, and the fingerprints associated with the innocent data at the server;

(d) receiving the subject data transmitted from the client computer in response to the request;

(e) analyzing the subject data transmitted from the client computer; and

(f) updating the fingerprints associated with the innocent data based on the analysis; wherein the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.